



#9  
10/3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 09/888,452  
Applicant: Gopalan  
Filing Date: 06/25/2001  
Group Art Unit: 2134  
Title: Apparatus and Method for Providing a Centralized Personal Database  
Accessed by Combined Multiple Identification Numbers

APPEAL BRIEF

RECEIVED

MAY 17 2004

Technology Center 2100

Mail Stop Appeal Brief – Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This Brief is support for the appeal in the above referenced application and is filed pursuant to the Notice of Appeal dated 4/29/2004. The Brief is submitted in triplicate.

The appeal brief fee of \$330 is to be charged to Deposit Account No. 09-0447 as indicated on the attached Fee Transmittal sheet.

05/13/2004 SSITHIB1 00000072 090447 09888452

01 FC:1401 330.00 DA

**REAL PARTY IN INTEREST**

The real party in interest in the present application is the following party: International Business Machines Corporation.

**RELATED APPEALS AND INTERFERENCES**

There are no appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

**STATUS OF CLAIMS**

**A. Total Number of Claims in the Application**

Claims in the application are: 1-26

**B. Status of all Claims in the Application**

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-26
4. Claims allowed: None
5. Claims rejected: 1-26

**C. Claims on Appeal**

The claims on appeal are: 1-26

**STATUS OF AMENDMENTS**

All of the amendments have been entered in the present case.

### **SUMMARY OF INVENTION**

The present invention is a centralized database that stores and communicates a consumer's personal information to a plurality of merchants. The personal information can include the consumer's name, address, telephone number, bank account information, credit card information, and so forth. The consumer accesses the database using a basic number and a primary number. Once accessed, the consumer configures the database by entering his personal information into the database. When configuring the database, the consumer creates a plurality of secondary numbers. Each secondary number specifies the information that the merchant will have access to in the database. In other words, each secondary number corresponds to a different level of access within the database. The consumer then issues the primary number and a secondary number to the merchants whom he wants to have his updated personal information. If desired, the consumer may also specify an expiration date or time period for any of the secondary numbers. The basic number, the primary number, and the secondary number are used by the consumer and the merchant to access the database as shown below:

<b>Type of Number</b>	<b>Consumer</b>	<b>Merchant</b>
Basic	Yes	No
Primary	Yes	Yes
Secondary	No <sup>1</sup>	Yes

In order to access the database, each merchant needs a primary number and a secondary number. The primary number is common to all merchants and is the same as the primary number that the consumer uses to access and modify the database. However, the secondary number may be different from merchant to merchant and controls how much information the merchant has access to. For example, a consumer may want his bank to have access to all of his

---

<sup>1</sup> The consumer creates the secondary number when configuring the database, but does not use the secondary number to access the database.

personal information, so he would issue a primary number and a secondary number to his bank. By contrast, the consumer may want his frequent flier program to have access to less information, so he would issue the same primary number and a different secondary number to his frequent flier program. Thus, the primary number identifies the consumer's personal information in the database and the secondary number identifies the merchant's level of access to the personal information in the database.

When the consumer updates his personal information and needs to notify the merchants of the change, he accesses the database and updates his personal information in the database. Only the consumer may modify the personal information because the basic number is required to modify the database. Once the update is completed, the database notifies the merchants that the consumer has changed his personal information and instructs the merchants to synchronize their records with the personal information in the database. The merchants may optionally schedule automatic synchronization with the database so that the merchant notification step can be eliminated. The merchants may access, but may not modify, the personal information in the database because they have the secondary number but not the basic number. The secondary number specifies the level of access that the merchants have within the database. Thus, the present invention allows a user to update his personal information with a plurality of merchants without having to send his personal information to each individual merchant.

### ISSUES

1. Does Card ([www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev\\_p.html](http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev_p.html), hereinafter Card) render claims 1-6 and 8-26 unpatentable under 35 USC §103(a) by teaching or suggesting a database that can be accessed and modified by a consumer using a basic number and

a primary number, and in which the database can be accessed, but not modified, by a merchant using the primary number and a secondary number?

2. Does Card render claim 7 unpatentable under 35 USC §103(a) by teaching or suggesting a database that allows a consumer to specifically designate merchant accessibility within the database by issuing different secondary numbers to a plurality of merchants?

3. Does Card contain a suggestion or motivation to modify the teachings of Card, one of the requirements of a *prima facie* case of obviousness under 35 USC §103(a)?

### **GROUPING OF CLAIMS**

Appellants expressly state that the claims do not all stand or fall together, for the reasons stated herein. For purposes of this appeal, the appellants have divided the claims into the following groups, the claims within each group being deemed to stand or fall together. However, in the event that new references are cited or new arguments advanced for rejection of the claims, appellants reserve the right to argue that additional claims do not stand or fall together.

Group I: Claims 1-6 and 8-26

Group II: Claim 7

### **ARGUMENTS**

**1. The Examiner must meet all three prongs of the obviousness test in order to establish a *prima facie* case of obviousness.**

The obviousness rejections are not well founded because the Examiner has not established a *prima facie* case of obviousness. The requirements for a *prima facie* case of obviousness are well defined:

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. MPEP §706.02(j) citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (emphasis added).

Similarly, the fact that the Examiner has the burden of proof with respect to the elements of the *prima facie* case of obviousness is also well defined:

To reject claims in an application under section 103, an examiner must show an un rebutted *prima facie* case of obviousness. In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *In re Rouffet*, 149 F.3d 1350, 1355, 47 USPQ2d 1453, 1457 (Fed. Cir. 1998).

With respect to claims 1-26, the Examiner has not met his burden of presenting the *prima facie* case of obviousness with respect to the first or third prongs of the obviousness test because Card does not teach or suggest the limitations of claims 1 and 7, and there is no suggestion or motivation to modify the teachings of Card to obtain the limitations of claims 1 and 7.

**2. The Examiner has not met his burden of presenting the *prima facie* case with respect to the third prong of the obviousness test because Card does not teach or suggest a database that can be accessed and modified by a consumer using a basic number and a primary number, and in which the database can be accessed, but not modified, by a merchant using the primary number and a secondary number.**

Claim 1 reads:

1. A programmable apparatus comprising:

...

wherein a consumer uses a basic number and a primary number to access an account in the data base and the consumer can modify an account data in the data base; and

wherein a merchant uses the primary number and a secondary number to

access the account and the merchant is prohibited from modifying the account data in the data base.

The Examiner rejected claims 1-6 and 8-26 under §103(a) as being unpatentable over Card. Specifically, the Examiner stated:

In regard to claim 1, Card teaches a programmable apparatus comprising:

...  
wherein a consumer uses a basic number and a primary number to access an account in the data base and the consumer can modify an account data in the data base (Section How to write a Java Card applet, i.e. electronic wallet application, access to the wallet is authenticated by an owner PIN)[;] and

wherein a merchant uses the primary number and a secondary number to access the account and the merchant [is prohibited] from modifying the account data in the data base (Section How to write a Java Card applet, i.e. electronic wallet application, access to the wallet is authenticated by an owner PIN). Office Action dated 12/03/2003, p. 3.

The section of Card cited by the Examiner reads:

The best way to determine how to create a Java Card 2.0 applet is to walk through an example. The following example is an electronic wallet application, which stores electronic cash. The wallet handles read\_balance, deposit, and debit APDU commands. Access to the wallet is authenticated by an owner PIN. Card, p. 7.

Clearly, the above section of Card does not teach or suggest the use of a three-number system for accessing and modifying account data in a database. In the third Office Action dated 4/5/2004, the Examiner offered more explanation:

The arguments can be summarized as: the three separate numbers of the claimed invention were not taught by the reference (Card). Yet, in the section "how to write a Java Card applet", this was clearly noted. For example, the read\_balance, deposit, and debit commands operate with the assumption that PIN is operational. The PIN is not [a] mere "personal identification number." See, for example, the code line using PIN:

```
byte byteRead=(byte)
(adpu.setIncomingAnd Receive());
```

Clearly, PIN class is a building block for Java Card program. A class may be used multiple times to produce objects. Thus, that there is one PIN class does not mean there is only one PIN object. Furthermore, in the section "The Java Card 2.0

framework”, the EMV standard is explicitly mentioned. Thus, the three numbers of the claims are suggested (by the EMV standard).

Thus, the claimed invention was taught by the cited reference. Office Action dated 4/5/2004.

In summary, the Examiner states that the PIN disclosed in Card is not a traditional personal identification number, such as those used for ATM cards and debit cards. The Examiner reasons that because the PIN can be used multiple times to create multiple PINs, the cited sections of Card teach or suggest the use of a three-number system for accessing and modifying account data in a database. This conclusion is clearly erroneous.

The Examiner states that the PIN disclosed in Card is not a personal identification number; however, all evidence point to the contrary. A traditional personal identification number, such as those used by ATM cards and debit cards, is generally a four digit number. Card defines the maximum size of PIN to be four digits:

//maximum size PIN  
final static byte MaxPin Size =(byte)0x04.<sup>2</sup> Card, p. 8.

As seen above, Card limits the PIN to a maximum size of four digits, just like a traditional personal identification number. Thus, the size of the PIN is identical to the size of a traditional personal identification number.

A second feature of a traditional personal identification number is that the traditional personal identification number is necessary to make an account transaction, such as a deposit, withdrawal, or balance inquiry. If the incorrect personal identification number is entered, then the transaction is rejected. Card states that the PIN must be validated before the user can make a deposit, debit, or get the account balance:

---

<sup>2</sup> When writing JAVA programs, numbers are typically expressed in their hexadecimal notation using the “0x” prefix followed by the two-digit number. Thus, “0x04” is the hexadecimal notation for the number “4.”



PIN is a method commonly used in smart cards to protect data from unauthorized access.

...

After the applet is successfully selected, PIN needs to be validated first, before any other instruction can be performed on the applet. Card, p. 12-13.

PIN validation means that the correct PIN must be entered. Failure to enter the correct PIN means that the deposit, debit, or balance applet will not run, just like a traditional personal identification number. Thus, the authorization feature of the PIN is identical to the authorization feature of a traditional personal identification number.

A third feature of a traditional personal identification number is that a predetermined number of incorrect personal identification number attempts will temporarily suspend the account and prohibit further personal identification number entry attempts. Card defines the maximum number of incorrect PIN entry attempts before the PIN is blocked:

A PIN records the number on unsuccessful tries since the last correct PIN verification. The card would be blocked, if the number of unsuccessful tries exceeds the maximum number of allowed tries defined in the PIN. Card, p. 12-13.

Card allows up to three incorrect PIN attempts before further PIN attempts are blocked, just like a traditional personal identification number. Thus, the security feature of the PIN is identical to the security feature of a traditional personal identification number.

The three above sections of Card are the only sections where the features of PIN are discussed. All of the PIN features are identical to the features of a traditional personal identification number. Therefore, the PIN in Card is identical to a traditional personal identification number.

The Examiner's assertion that the PIN is a class that can be used to produce multiple objects further supports the fact that PIN is a traditional personal identification number. The methods used to produce traditional personal identification numbers may be repeated to produce

a plurality of different traditional personal identification numbers. While the actual numbers may be different (i.e. 1111, 2222, 3333, or 4444), their function remains the same: the personal identification number is used to verify authorization to access and provide security for the account. Similarly, the PIN applet in Card may be used to produce multiple PINs; however, the function of each PIN is identical: the PIN is used to verify authorization to access the account.

By contrast, the present invention utilizes three distinctly different numbers to determine whether the accessing party can modify the account data in the database. The consumer uses both the basic number and the primary number to access the account data in the database. The primary number identifies the consumer and the basic number authorizes the consumer to modify the database. Once the consumer has accessed the account data, the consumer can modify the account data without any restrictions. On the other hand, the merchants use both the primary number and the secondary number to access the account data in the database. The primary number identifies the consumer and the secondary number designates the level of access within the database. Once the merchant has accessed the account, the merchant may not modify any of the personal information in the account. These limitations are captured in the following claim limitations: “wherein a consumer uses a basic number and a primary number to access an account in the data base and the consumer can modify an account data in the data base;” and “wherein a merchant uses the primary number and a secondary number to access the account and the merchant is prohibited from modifying the account data in the data base.” These limitations are not taught or suggested by Card. Therefore, the claims of Group I should be allowed over the cited prior art.

**3. The Examiner has not met his burden of presenting the *prima facie* case with respect to the third prong of the obviousness test because Card does not teach or suggest a database that allows a consumer to specifically configure merchant accessibility within the database by issuing a different secondary number to each individual merchant.**

Claim 7 reads:

7. The programmable apparatus of claim 1 wherein the database further comprises a secondary number generation program comprising:

...  
instructions for consumer designation of an information to be accessed by the merchant ...

The Examiner rejected claim 7 under §103(a) as being unpatentable over Card.

Specifically, the Examiner stated:

Regarding claims 3, 5, 7, 8, 11, 12, 25, such handling of consumers by such particular uses of basic, primary and secondary numbers in such particular ways are suggested by Card (Section What is a Java Card, Subsection The lifetime of a Java Card, i.e. discussion on personalization of consumer data – which permits consumers to use such data). Office Action dated 12/3/2003, p. 4.

The Examiner offered no further explanation for the rejection of claim 7.

The section of Card cited by the Examiner reads:

The Java Card lifetime starts when the native OS, Java Card VM, API classes libraries and optionally, applets are burned into ROM. This process of writing the permanent components into the non-mutable memory of a chip for carrying out incoming commands is called masking.

Before it lands in your wallet, a Java Card needs to go through initialization and personalization. Initialization refers to loading general data into a card's non-volatile memory. This data is identical across a large number of cards and is not specific to an individual; an example might be the issuer or manufacture's [sic] name.

The next step, personalization, involves assigning a card to a person. It can occur through physical personalization or through electronic personalization. Physical personalization refers to embossing or laser engraving your name and card number on the plastic surface of the card. Electronic personalization refers to loading personal data into a card's non-volatile memory, for example, your personal key, name, and pin number.

Initialization and Personalization vary from vendor to vendor and issuer to issuer. In both, EEPROM (a type of non-volatile memory) is often used for storing data.

At this point, the Java Card is ready for use. You can get a Java Card from an issuer or buy it from a retailer. Cards sold by a retailer are general-purpose, in which case personalization is often omitted.

Now you can insert your Java Card into a reader and send APDU commands to the applets residing on the card or download more applets or data onto the card.

A Java Card remains active until it is expired or blocked due to an unrecoverable error. Card, p. 4-5.

The above section of Card does not relate to the claimed limitations in any way. The above section of Card refers to the process of setting up the Java Card (Initialization) and the process of personalizing the card to a specific user (Personalization). Card does not teach or suggest a method by which the consumer can designate the information that the merchant has access to in the above section or any other section of Card. Because Card does not teach or suggest the claimed limitation, the claim of Group II should be allowed over the above prior art.

**4. The Examiner has not met his burden of presenting the *prima facie* case with respect to the first prong of the obviousness test because Card does not contain a suggestion or motivation to modify the teachings of Card to obtain the claimed invention.**

As stated in part 1, *supra*, in order for the Examiner to make out a *prima facie* case of obviousness under 35 USC §103(a), the Examiner must identify some suggestion or motivation to modify the reference to obtain the claimed invention. "Even when obviousness is based on a single prior art reference, there must be a showing of a suggestion or motivation to modify the teachings of that reference." *In re Kotzab*, 217 F.3d 1365, 1370, 55 U.S.P.Q.2d 1313, 1318 (Fed. Cir. 2000). With respect to the claims 1 and 7, the Examiner has not provided any motivation whatsoever for modifying the teachings of Card to obtain the claimed invention. Absent a showing of the motivation to modify, the Examiner cannot make out a *prima facie* case of obviousness. Consequently, the claims of groups I and II should be allowed over the prior art.

For the foregoing reasons, the Applicant submits that the claims of the present application are not fairly taught by and are not obvious in light of, any of the references of record taken either alone or in combination. Therefore, allowance of the present application is in order, and is requested.

Respectfully submitted,



Rudolf O. Siegesmund  
Registration No. 37,720  
Suite 2000  
4627 N. Central Expressway  
Dallas, Texas 75205-4017  
214-528-2407  
FAX 214-528-2434  
Attorney for Applicant

**Certificate of Express Mail**

Express Mail Label No. ER392173263US Date of Deposit: 5/11/04

I hereby certify that this paper and fee are being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



Rudolf O. Siegesmund

**APPENDIX**

The text of the claims involved in the appeal is:

1. A programmable apparatus comprising:
  - a data base in a first computer;
  - a network;
  - a second computer connected to the first computer by the network;
  - wherein a consumer uses a basic number and a primary number to access an account in the data base and the consumer can modify an account data in the data base; and
  - wherein a merchant uses the primary number and a secondary number to access the account and the merchant is prohibited from modifying the account data in the data base.
2. The programmable apparatus of claim 1 further comprising synchronization of data between the second computer and the first computer, said synchronization being a transfer of the account data from the data base to the merchant at a pre-arranged time and a pre-arranged schedule.
3. The programmable apparatus of claim 1 further comprising data transmitted from the first computer to the second computer in response to receipt of a basic number and the primary number by the first computer; and wherein the second computer is a consumer computer.
4. The programmable apparatus of claim 1 further comprising data transmitted from the first computer to the second computer in response to receipt of the primary number and the secondary number by the first computer; and wherein the second computer is a merchant computer.
5. The programmable apparatus of claim 1 wherein the data base further comprises a computer implemented process comprising:

consumer registration with the data base;

merchant notification of the consumer registration; and

updating merchant records using information stored in the data base.

6. The programmable apparatus of claim 1 wherein the data base further comprises a merchant access program comprising:

instructions for verifying correct entry of the primary number and the secondary number by the merchant;

instructions for allowing the merchant to search for information in the account; and

instructions for allowing the merchant to synchronize the information in the data base with the merchant's records.

7. The programmable apparatus of claim 1 wherein the data base further comprises a secondary number generation program; comprising:

instructions for consumer access to the account using the basic number and the primary number;

instructions for consumer designation of an information to be accessed by the merchant;

instructions for creation of the primary number and the secondary number; and

instructions for transmitting the primary number and the secondary number to the merchant.

8. The programmable apparatus of claim 1 wherein the data base further comprises a registration program comprising:

instructions for allowing the consumer to register the account with the data base;

instructions for accepting consumer input of data into the account; and

instructions for issuing the basic number and the primary number to the consumer.

9. The programmable apparatus of claim 1 wherein the data base further comprises a merchant notification program comprising:

instructions for determining whether the merchant has been added to the data base;

responsive to a determination that the merchant has not been added to the data base,

instructions for adding a merchant to the data base;

instructions for associating a merchant with data in the account, a primary number, and a secondary number; and

instructions for sending the primary number and the secondary number to the merchant.

10. The programmable apparatus of claim 1 wherein the data base further comprises a merchant data base.

11. The programmable apparatus of claim 1 wherein the data base further comprises a consumer data base.

12. The programmable apparatus of claim 1 wherein the data base may be accessed by the consumer using the basic number and the primary number; and wherein the consumer is the only party who may modify the data in the data base.

13. The programmable apparatus of claim 1 wherein the data base may be accessed by the merchant using the primary number and the secondary number; and wherein the secondary number is unique to the merchant and distinguishes the merchant from a plurality other merchants.

14. A data base that may be accessed by a consumer having a basic number and a primary



number and by any party to whom the consumer provides the primary number and a secondary number; and wherein the primary number and secondary number are specific to each individual party to whom the consumer provides the primary number and the secondary number.

15. The data base of claim 14 wherein the data base may be accessed through the Internet from a data base web site.

16. The data base of claim 14 wherein the data base is located in one storage area connected to one or more server computers.

17. The data base of claim 14 wherein the data base is distributed in multiple storage areas each of which are connected to one or more server computers.

18. A method for remotely providing personal information from a data base comprising the steps of:

registering with the data base;

obtaining a primary number and a secondary number;

providing a person to whom access is desired with a primary number and a secondary number;

wherein the primary number and the secondary number allow access to the data base;

wherein the primary number and the secondary number prohibit modification to the data base; and

wherein the primary number and secondary number are specific to each individual person to whom the consumer provides the primary number and the secondary number.

19. The method of claim 18 further comprising the step of accessing.

20. The method of claim 18 further comprising the step of creating the secondary number.
21. The method of claim 18 further comprising the step of selecting information to be accessed by a combination of the secondary number and the primary number.
22. The method of claim 18 further comprising the step of synchronization.
23. A computer readable memory comprising:
  - a computer readable storage medium;
  - a data base in said computer readable memory;
  - a computer program stored in said storage medium;wherein the storage medium, so configured by the computer program, allows access to, but not modification of, the data base upon receipt of a correct combination of a primary and a secondary number.
24. The programmable apparatus of claim 6 wherein the merchant access program further comprises: instructions for allowing a merchant to designate whether the synchronization is immediate or scheduled.
25. The programmable apparatus of claim 7 wherein the secondary number generation program further comprises: instructions for consumer designation of an expiration date for the secondary number.
26. The programmable apparatus of claim 1 wherein the data base is accessed through the Internet through a centralized personal data base web site; and wherein the data base is located in a storage area connected to one or more server computers that may be distributed in multiple storage areas each of which are connected to one or more server computers.